(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 0 485 090 B1

(12) **EUROPEAN PATENT SPECIFICATION**

(45) Date of publication and mention of the grant of the patent:
06.05.1998 Bulletin 1998/19

(51) Int Cl.[6]: **G07F 7/08**

(21) Application number: **91309894.3**

(22) Date of filing: **25.10.1991**

(54) **Transaction approval system**

Transaktionsgenehmigungssystem

Système d'acceptation de transactions

(84) Designated Contracting States:
AT BE CH DE DK ES FR GB GR IT LI LU NL SE

(30) Priority: **09.11.1990 US 611933**

(43) Date of publication of application:
13.05.1992 Bulletin 1992/20

(60) Divisional application: **95202930.4 / 0 709 811**

(73) Proprietor: **VISA INTERNATIONAL SERVICE ASSOCIATION**
San Mateo California 94402 (US)

(72) Inventor: **Adams, Carl A.**
San Francisco, California 94133 (US)

(74) Representative: **Jackson, David Spence et al**
REDDIE & GROSE
16, Theobalds Road
London, WC1X 8PL (GB)

(56) References cited:
EP-A- 0 088 639
EP-A- 0 107 865
EP-A- 0 127 424
EP-A- 0 200 343
EP-A- 0 349 413
GB-A- 2 151 061
US-A- 4 718 009
US-A- 4 727 243
US-A- 4 874 932
US-A- 4 891 503

EP 0 485 090 B1

Printed by Jouve, 75001 PARIS (FR)

Description

This invention relates to a system for authorising transactions, and to a method for adjusting the transaction limit in a terminal.

A large percentage of transactions are now completed using a transaction card, rather than cash or checks. A small but significant percentage of all such transactions generate losses due to improper usage of the cards. Such improper usage can include exceeding the credit limit of the card. The definition of improper use also includes continued purchasing while failing to pay monthly minimum charges. Various fraud scenarios also contribute to this loss. For example, purchases are made with cards that have been lost or stolen. In addition, dishonest employees at a merchant can improperly create a transaction through the unauthorised use of an account number.

Many approaches have been implemented to reduce these losses. One of the earliest approaches used to combat these losses was to distribute a printed list of invalid cards. In use, the merchant would check the account number on the card presented for the transaction with the account numbers printed in the list. If the account number is listed, the transaction would be declined.

The use of such a printed list is effective in reducing a large percentage of fraud losses. Unfortunately, this approach has a few drawbacks. For example, a transaction card is often used almost immediately after it has been lost or stolen. This immediate use will occur before the card has been listed or before the list has been distributed.

Because of these difficulties, other, more sophisticated techniques have been implemented. One of the most effective schemes is to authorize every transaction through a real-time, on-line communication network. For example, an automated transaction terminal at the merchant can transmit the account number of the card presented for a transaction to a central processor. The account number of the card can then be checked against a current list of invalid card numbers stored either at the central processor or back at the card issuer.

This on-line scheme eliminates the lag time inherent in distributing printed lists of invalid cards. Furthermore, the cost of authorizing transactions is justified for high value transactions. However, for low value transactions, the losses tend to be lower and the benefits gained from on-line authorization do not justify the added costs and delay involved in obtained an on-line approval.

Accordingly, various approaches have been developed to authorize lower value transactions at the terminal, in an off-line manner. The simplest approach has been to provide the terminal with a transaction or "floor" limit. Any transaction having a value which is below that floor limit can be approved by the terminal. If the value of the transaction exceeds that floor limit, a request for authorization must be generated and transmitted to the central processor.

The floor limit selected for a particular terminal has traditionally been based on the type of merchant establishment and its location. The floor limit selected represents an attempt to balance the level of loss which will occur for transactions that are authorized by the terminal with the cost of transmitting the requests to the central processor.

In most systems, the issuer of the card has no control over the floor limit. More recently, a system has been developed wherein both the issuer and the financial institution that supplies the terminal to the merchant have a say as to the floor limit in the terminal. Such a system is described in European Patent No. 0 200 343.

In this system, the terminal determines the transaction limit using data both stored in the terminal and data encoded on the transaction card.

The data in the terminal used to calculate the transaction limit is also determined by the type and location of the merchant. This information is fixed in the terminal. While this approach successfully reduces some fraud losses, it cannot accommodate short term changes in the patterns of loss which occur at a specific terminal. For example, if a new employee is dishonest or follows sloppy procedures, the losses will immediately increase. Accordingly, it would be desirable to actively update the transaction limit in the terminal to maintain the desired balance between the level of risk and communication costs.

Another approach for reducing losses when a terminal authorizes transactions in an off-line mode is to provide the terminal with a list of invalid account numbers. Such a system was disclosed in U.S. Patent No. 3,696,335, issued October 3, 1972 to Lemelson. The latter approach required that the entire list of invalid cards be transmitted to the terminals. This approach has been found to be impractical because the list is quite long and therefore requires large data storage capacity in the terminals. The list would also take a long time to transmit to the terminals.

Various suggestions have been made to overcome these problems. For example, U.S. Patent No. 4,558,211, issued December 10, 1985 to Berstein teaches that the list can be reduced by geographical criteria.

Still another approach which has been suggested is disclosed in U.S. Patent No. 4,943,707, issued July 24, 1990 to Boggan, and incorporated herein by reference. In this patent, a system is disclosed for generating a data compressed version of the invalid card list. This data compressed version is much shorter and therefore requires less storage space in the terminal and can be transmitted faster. However, in certain cases, the cost of this approach still exceeds the benefits gained in reduction of loss. Accordingly, it would be desirable to provide other techniques for storing lists of potentially invalid cards which is not subject to any of the draw-

backs discussed above.

Therefore, it is an object of the subject invention to provide an improved transaction approval system.

It is another object of the subject invention to provide a transaction terminal with enhancements for improving the effectiveness of the authorization process.

It is a further object of the subject invention to provide a transaction approval system wherein the transaction limit in the terminal can be varied.

It is still another object of the subject invention to provide a transaction approval system wherein the transaction limit in the terminal can be adjusted to reflect a desired level of risk of loss.

The present invention is defined by claims 1 and 7 hereinafter, to which reference should now be made.

The dependent Claims define further embodiments of the invention.

In a preferred embodiment of the invention, long term and short term transaction histories are monitored.

A certain amount of memory in the terminal can be devoted to storing account numbers which will provoke a request for on-line authorization information. The account numbers are stored in three different lists. The first list is generated by the central processor and transmitted to the terminal. This list includes specific invalid account numbers. This list can be a data compressed version of an invalid card list described above with respect to U.S. Patent No.4,943,707. The list is very short and includes only those invalid cards which had been reported actually used in the narrow geographical region where the terminal is located.

The second and third lists are generated locally at the terminal and are based on activity at that terminal. The second list includes a record of account numbers from transactions that were forwarded to the central processor for authorization information and the central processor declined the transaction. Since this card is identified as at least suspicious, any subsequent uses should provoke an on-line request even if the transaction amount is below the transaction limit of the terminal. By placing the card on the second list, such an on-line request will be generated.

The third list contains account numbers of cards for transactions where the transaction amount was below the transaction limit and was approved, off-line by the terminal. Once the account number is placed on this list, any subsequent uses of the card at that terminal will provoke an on-line request. This technique is intended to frustrate the fraud scenario wherein the card is repeatedly used for many low value transactions in an effort to avoid detection.

It should be noted that the concept of adding account numbers to a terminal to provoke an on-line request for authorization during a subsequent use is disclosed in the above cited U.S. Patent No.4,943,707. However, in the system described in the latter patent, the account number was always added to the list if it had not been present in the list previously, regardless of whether the transaction was approved off-line. Thus, even if the transaction was forwarded for on-line authorization because, for example, the transaction amount exceeded the transaction limit, the account number was still added to the list. It is believed that the latter approach is not as efficient as that described herein where the account number is added to the list only if the transaction is approved off-line by the terminal.

Further objects and advantages of the subject invention will become apparent from the following detailed description taken in conjunction with the following drawings in which:

Brief Description of the Drawings:

Figure 1 is a block diagram of a transaction approval network of the subject invention.

Figure 2 is a flow chart illustrating the steps performed during a transaction in a terminal operating in accordance with the subject invention.

Detailed Description of the Preferred Embodiment

Referring to Figure 1, there is illustrated an overall block diagram of a transaction approval network 10. The network 10 includes a central processor 12 which functions as communication node between financial institutions that issue transaction cards (issuers 14) and terminals 16. As shown in Figure 1, the terminals 16 can be directly connected to the central processor 12. In large transaction systems, there exists intermediate financial institutions and processors which act as intermediate communication nodes. For the purposes of describing the subject invention, the intermediate communication nodes can be considered transparent to the system.

In existing systems, the central processor can route requests for authorization information generated at a terminal 16 to the issuer 14 of the transaction card. The issuer will determine if a particular transaction can be approved. An appropriate response is generated by the issuer and transmitted back to the terminal.

If the issuer is unavailable, the central processor will act on the authorization request. To facilitate the evaluation of the transaction, the central processor maintains a list 20 of invalid cards, generated from information supplied by the issuers. The central processor consults that list in determining whether a particular transaction can be approved.

As noted above, many existing transaction terminals are equipped to authorize a certain percentage of transactions in an off-line manner, without contacting the central processor. These existing terminals includes internal processors and electronic memories. The design of such terminals is well known to those skilled in the art and need not be discussed. The subject invention can be implemented in latter type of terminals with the modifications discussed below.

In order to authorize the transaction locally, an existing terminal will carry out a number of tests. For example, the terminal will determine if the card has expired by comparing the expiration date to the current date. The terminal can also determine if the account number is in an allowable format so that forged cards can be identified.

The terminal will also determine if the transaction amount is below an internally set transaction limit. If the transaction amount exceeds the transaction limit, a request for authorization information will be generated and transmitted to the central processor. The central processor will supply a response to the terminal, based on information from its own data base or based on a communication with the issuer. If the transaction amount is below the transaction limit, then the terminal can authorize the transaction.

As noted above, the transaction limit is typically fixed in the terminal. It is selected to control the risk of loss at a desired level. Terminals which are in locations which are subject to high loss will have a low transaction limit. If losses are very high, the transaction limit could even be set to zero to insure that all transactions are sent on-line for authorization. In contrast, terminals which are located at merchants where losses are low can have a high transaction limit, such as $50 or more.

As noted above, the loss associated with low value transactions is not high. It has been determined that the average additional loss which can be expected when a twenty dollar purchase is not authorized in an on-line manner amounts to about four cents. In contrast, it costs about ten cents to obtain an on-line authorization. Thus, as long as the rate of risk of additional loss is maintained at a low level, it will be more cost effective to authorize low value transactions off-line. This goal can be achieved by dynamically adjusting the transaction limit in the terminal. The subject approach has the added benefit that off-line approvals are much faster and therefore highly desirable in high volume, low value environments.

As noted above, in the prior art systems, the transaction limit was selected and stored in the terminal based on past performance by the merchant and the location of merchant. It is believed that at least one system exists where the transaction limit can be downloaded to the terminal from a central source. However, even in the latter system, the criteria for selecting the transaction limit is only based on regional statistics. No effort is made to analyze the performance of specific terminals. Accordingly, no prior art system could respond to a change in the level of risk at a particular terminal. Such a change could result from the hiring of a dishonest employee.

The transaction limit in the terminal can be dynamically varied to maintain the desired balance between the level of risk and communication costs. In order to carry out this goal, the central processor must assess the transaction history at the terminal on a regular basis and compute the actual level of risk associated with those transactions.

There presently exists transaction terminals which keep a record of all transactions. These terminals are referred to as data capture terminals. The transaction records are collected in a memory 28 and typically downloaded to the central processor, once a day, in a batch process. This information is used by the central processor to generate billing information which is then supplied to the respective issuers. The card issuers will then generate the bills that will be sent to the cardholder.

As can be seen, a mechanism already exists for communicating the transaction records to the central processor. The central processor will now determine the number of transactions which have occurred at that terminal that are based on accounts in the master invalid card list 20. While debts created during many of these transactions will be ultimately collected, the likelihood that the debt will be uncollectible is quite high. If the level of risk posed by these recorded transactions differs from the desired level, the central processor can calculate a new transaction limit intended to adjust the level of risk to be closer to the desired level. This new transaction limit is then downloaded to the terminal and is stored in memory 30. The downloading process can be carried out during the existing data capture communication sessions.

The central processor will store in memory 32, a record of the existing transaction limit for each terminal. The memory will also keep a record of both the long and short term history of the risk level at the terminal. For example, the processor will keep a count of the number of transactions at the terminal and the number of improper card usages. The short term count will keep a rolling total for several days, while the long term count will cover several weeks. Both of these records are updated each time data is received from the terminal.

The analysis will be performed on all transactions, even those that were authorized on-line. In this manner, the system can detect an improper transaction that might have been approved on-line. The latter situation can occur if the transaction took place before a card was reported lost or stolen but was subsequently reported prior to the analysis by the central processor.

The calculation process by the central processor will be based on a table of decision rules. If both the long and short term risk level are below a threshold, the transaction limit could be increased. If either or both the long and short term risk level are above a threshold, the transaction limit can be adjusted downwardly. If it is determined that a new limit is necessary, that information can be downloaded to the terminal and recorded at the central processor during the next data capture session.

In order to minimizes losses for transactions that have a value below the transaction limit, it is desirable to add procedures that will provoke a request for on-line authorization in situations where there is a heightened possibility that the transaction is fraudulent. One method

that has been suggested is to generate an on-line request for authorization when the value of the transaction falls in a small range just under the transaction limit. This approach can be used to prevent someone who has knowledge of the transaction limit from avoiding detection by restricting the value of purchases to amounts slightly less than the transaction limit.

Another approach is to provide the terminal with a list of invalid cards. Various methods have been developed to carry out this approach as disclosed in the above cited patents. Most of these approaches require a large amount of memory in the terminal. In addition, transmission of such lists takes a significant amount time. In the subject system, an attempt is made to derive similar benefits while reducing the memory storage and communication requirements.

In the system, the terminal is further provided with a memory area 40 for storing lists of suspect cards. The account number of each card presented for the transaction is compared to the account numbers in these lists. If the account number is present, the terminal will generate a request for authorization information from the central processor.

Memory area 40 is subdivided into three lists. The first list 42 is generated by the central processor 12 and supplied to the terminal 16. This list contains invalid account numbers and could be in the form described in EP-A-200343. However, the data compressed master table described in the latter patent might hold information about 100,000 invalid accounts and require 125 kilobytes of memory. In the subject system, it is desirable that the entire memory 40 be only about 5 kilobytes in length. Various data compression algorithms can be used to maximize the storage capability of this memory space.

The list generated by the central processor should be limited to a small subset of invalid cards that have been reported actually used in the narrow geographical area where the terminal is located. In addition, this list can be limited to cards that have been used in this type of terminal , which, as noted above, will most likely be placed in high volume, low value environments. As noted above, the subject invention includes a mechanism for daily reporting all of transaction activity from data capture terminals to the central processor. Thus, the central processor can compare the transaction records with its list of invalid cards and accurately compile a list of fraudulent cards that were used in a given region.

Since the regional list compiled by the central processor is limited to cards actually used it will be relatively small and can be transmitted quickly. Transmission time is further reduced by only transmitting new account numbers that appear on the list. These entries can be added to the list 42 in the terminal. When the region in memory storing the list is full, the oldest entry in terms of time can be deleted to make room for the most recent entry. Preferably, the parameters of the system are arranged such that any entry will remain resident in the terminal an average of about three weeks.

The remaining two regions in memory 40 include lists which are generated by and remain in the terminal. List 44 contains a list of accounts numbers which are associated with a transaction that provoked an on-line request for authorization information and the response from the central processor was to decline the transaction. In this case, the account number is clearly suspect and any future use of the card should be scrutinized. By placing the account number on this list, an on-line request will be generated for each subsequent use of the account number even if the transaction amount is below the transaction limit. As with the first list 42, when the memory space is full, the oldest entry can be deleted to make room for the most current entry.

The third list 46 contains account numbers of all cards which have been involved in transactions that have been approved off-line. By this approach, the second use of the card at that terminal will provoke an on-line request for authorization information. The system will therefore allow a single fraudulent use below the transaction limit but will stop a second use. It has been found that a common fraudulent activity pattern includes multiple low value transactions at a single terminal. Recording account numbers associated with transactions that have been approved off-line will prevent such a fraud scenario. Once again, when the list is full, the oldest entry can be deleted to make room for the most current entry.

While multiple uses of a card at a single terminal for low value transactions is often associated with fraudulent activity, it is also quite common and legitimate in certain merchant situation. For example, a number of "fast food" restaurants are beginning to accept transaction cards for payment. It is not unusual for a customer to purchase food more than once a week from such a local establishment.

In order to reduce the number of times such additional low value transactions provoke an unnecessary on-line request for authorization, each account number in file 46 can further be provided with a data field indicating either the number of times it has been used or the date it was last used. If the data field is a usage counter, the requests for on-line authorization can be made only during the second usage or for every other usage. If the data field indicates the date it was last used, an on-line request can be generated only if the last use was relatively recently.

It should be understood that each terminal 16 can be provided with its own individual storage area 40. Alternatively, a single storage area 40 may be shared by a group of terminals at a given merchant location.

Figure 2 is a flow chart illustrating the steps taken at a terminal 16 to authorize a transaction. At the start of the transaction, the card is swiped through the terminal so that identifying information encoded on the magnetic stripe of the card can be read by the terminal. The merchant will also enter the amount of the transaction.

In step 50, the terminal will carry out a number of initial tests to determine if the transaction can be approved. As noted above, these tests will include a determination as to whether the card has expired. Assuming the initial hurdles are cleared, the terminal will compare the transaction amount to the transaction limit stored in memory 30 (step 52). In the preferred embodiment, the transaction limit is dynamically adjusted on a regular basis by the central processor to maintain the level of risk close to the desired level.

If the transaction amount exceeds the transaction limit, the terminal will generate and transmit a request for authorization information from the central processor in step 54. As noted above, either the central processor 12 or the issuer 14 of the card will generate a response. In either case, a response will received by the terminal in step 56.

The terminal will then determine if the transaction has been approved or declined in step 58. If it has been approved, the transaction can be completed in step 60. Typically a message which authorizes a transaction will include an authorization code which is recorded on the transaction receipt.

If the transaction has been declined, the transaction will not be completed. In addition, the account number will be recorded in list 44 (step 62). By this arrangement, the next usage of that account number will provoke an on-line request for authorization even if the transaction amount is below the transaction limit.

Returning to step 52, if the transaction amount does not exceed the transaction limit, then the terminal must determine if the account number is present on any of the lists stored in memory 40 (step 64). If the account number is present, the terminal will generate a request for on-line authorization in step 54. The terminal will then follow the sequence described above.

If the account number did not appear on any of the lists in memory 40, then the transaction can be completed and approved off-line in step 66. In this case, the terminal will generate an authorization code which is recorded on the transaction receipt. In accordance with the subject invention, since the transaction has been approved off-line, the account number will also be added to list 46 so that a subsequent use of the card will provoke an on-line request for authorization information (step 68). As noted above, the terminal will keep a record of all transactions, whether they were authorized or declined.

In summary, the transaction limit stored in the terminal can be dynamically adjusted to vary the level of risk at the terminal to be closer to the desired level of risk; and the terminal will generate and store a list of account numbers which might be invalid and should provoke an on-line request for authorization.

Claims

1. A system for authorising transactions, the system comprising a transaction approval network (10) having central processor means (12) for receiving and analysing transaction records for each of a plurality of remote transaction terminals (16) adapted to communicate with the central processor means (12) through the network (10), each transaction terminal (16) being adapted to authorise in an off-line mode transactions which satisfy tests carried out by the terminal (16) on the basis of authorisation information maintained in storage means provided therefor, and the terminal (16) being further adapted to store in the storage means a record of the transactions handled by the terminal (16) and having transmitting and receiving means associated therewith for receiving information from and transmitting information to the central processor means (12), the information transmitted to the central processor means (12) including the record of transactions at the terminal (16), and the central processor means (12) being adapted to control the off-line mode of each terminal (16) by calculating a level of risk associated with the transactions record of the terminal (16) and, if the calculated level of risk differs from a desired level of risk, transmitting to the terminal (16) new off-line mode transaction authorisation information selected to adjust the level of risk at the terminal (16) towards the desired level of risk.

2. A system according to claim 1, characterised in that said central processor means (12) calculates for each terminal (16) the level of risk over two time intervals of differing length to determine whether the off-line mode transaction authorisation information should be changed.

3. A system according to claim 1, characterised in that the central processor means (12) calculates the level of risk for each terminal (16) by comparing the transactions record of the terminal (16) with information about accounts associated with the transactions in the record.

4. A system according to claim 1, characterised in that the network (10) is adapted to operate in response to the use of transactions cards, each transaction card having an account number, and in that each terminal (16) is such that one of the said tests (64) comprises carrying out a comparison of the transaction amount presented for a transaction with a transaction limit included in the authorisation information and, if the transaction amount exceeds the transaction limit, the terminal (16) transmits a request for authorisation to the central processor means (12), and if such request for authorisation is declined, the terminal (16) adds the account

number of the transaction card presented for that transaction to a list (44) stored in said storage means (40).

5. A system according to claim 4, characterised in that each terminal (16) is such that one of the said tests (64) comprises comparing the account number of a transaction card presented for a transaction with the said list (44) and a further list (46) of account numbers of transaction cards, said further list (46) being stored in said storage means (40), and that, if (52) the transaction amount is not greater than the transaction limit included in the said authorisation information and (64) the account number of the presented transaction card is not present in the said lists, the terminal (16) adds (68) the account number of the transaction card presented for that transaction to said further list (46) in said storage means (40) so that a subsequent use of that transaction card at that terminal (16) will result in the terminal (16) transmitting a request for authorisation to said central processor means (12).

6. A system according to claim 4 or 5, characterised in that each terminal (16) is such that the maximum number of cards which can exist in the list is fixed and when that limit is reached, the account number oldest in the list is deleted to provide room for the next account number to be added to the list.

7. A method of operating a system for authorising transactions, the system comprising a transaction approval network (10) having a central processor (12) communicating with a plurality of remote transaction terminals (16), the method comprising performing for each terminal (16) the steps of:

receiving and storing at the location of the remote terminal (16) authorisation information for off-line mode transactions;
operating the terminal (16) in an off-line mode to authorise a transaction thereat if the transaction satisfies tests carried out by the terminal (16) on the basis of the stored authorisation information;

and controlling the off-line mode of operation of the terminal (16) by the steps of:

producing at the terminal (16) a record of transactions handled by the terminal (16);
transmitting the transactions record from the terminal (16) to the central processor (12); and
calculating at the central processor (12) a level of risk associated with the transactions record received from the terminal (16), and if the calculated level of risk differs from a desired level of risk, transmitting to the terminal (16) new off-line mode transaction authorisation information selected to adjust the level of risk at the terminal (16) towards the desired level of risk.

8. A method according to claim 7, characterised in that the level of risk is calculated over two time intervals of differing length to determine whether the transaction limit should be changed.

9. A method according to claim 7, characterised in that the level of risk is calculated by comparing the transactions record with information about accounts associated with the transactions.

10. A method according to claim 7, characterised in that transactions are authorised on the basis of the use of transactions cards, each transaction card having an account number; and in that for each remote terminal (16):

the authorisation information stored at the location of the terminal (16) includes a plurality of lists (42,44,46) of account numbers;

and the operation at the terminal (16) includes the steps of:

comparison of the account number of the card presented for a transaction with a first stored list (42) of invalid account numbers;
requesting authorisation from the central processor (12) for transactions which do not satisfy certain tests (52,64) based on the stored authorisation information, including a test (64) for absence of the account number in a second stored list (44);
and, if any such request for authorisation is declined (58), adding the account number of the transaction card presented for that transaction to the said second stored list (44) so that a subsequent use of that transaction card at the terminal (16) will result in the terminal (16) going on-line to request authorisation from the central processor (12) even if the remainder (50,52) of the tests based on authorisation information are satisfied.

11. A method according to claim 10, characterised in that the operation at each terminal (16) includes the step of:

if all the tests (50,52,64) based on authorisation information stored at the terminal (16) are satisfied, adding the account number of the transaction card presented for that transaction to a third stored list (46) so that a subsequent use of that transaction card at that terminal will result in the terminal going on-line to request authorisation from the central processor (12) if the remainder (50,52) of the tests based on authorisation information are satisfied, the said tests including a test (64) for absence of

the account number in the third stored list (46).

12. A method according to any one of claims 7 to 11, characterised in that the authorisation information includes a transaction limit and in that the selection of the said new off-line mode transaction authorisation information comprises calculation of a new transaction limit that adjusts the level of risk at the terminal (16) towards the desired level of risk.

Patentansprüche

1. System zum Genehmigen von Geschäften, mit einem Geschäftsgenehmigungsnetzwerk (10), das eine zentrale Prozessoreinrichtung (12) hat zum Empfangen und Analysieren von Geschäftsaufzeichnungen für jedes von mehreren entfernten Geschäftsterminals (16), welches in der Lage ist, mit der zentralen Prozessoreinrichtung (12) über das Netzwerk (10) zu verkehren, wobei jedes Geschäftsterminal (16) in der Lage ist, in einer Off-Line-Betriebsart Geschäfte zu genehmigen, die Tests bestehen, welche durch das Terminal (16) auf der Basis von Genehmigungsinformation durchgeführt werden, die in einer dafür vorgesehenen Speichereinrichtung aufbewahrt werden, und wobei das Terminal (16) weiter in der Lage ist, in der Speichereinrichtung eine Aufzeichnung der Geschäfte zu speichern, die durch das Terminal (16) gehandhabt werden, und mit einer zugeordneten Sende- und Empfangseinrichtung versehen ist, um Information aus der zentralen Prozessoreinrichtung (12) zu empfangen und zu dieser zu senden, wobei die zu der zentralen Prozessoreinrichtung (12) gesendete Information die Aufzeichnung von Geschäften in dem Terminal (16) umfaßt und wobei die zentrale Prozessoreinrichtung (12) in der Lage ist, den Off-line-Betrieb jedes Terminals (16) zu steuern, indem sie einen Risikowert berechnet, der der Geschäftsaufzeichnung des Terminals (16) zugeordnet ist, und, wenn sich der berechnete Risikowert von einem gewünschten Risikowert unterscheidet, eine neue Offline-Betriebsart-Geschäftsgenehmigungsinformation zu dem Terminal (16) zu senden, die so ausgewählt ist, daß der Risikowert in dem Terminal (16) auf den gewünschten Risikowert eingestellt wird.

2. System nach Anspruch 1, dadurch gekennzeichnet, daß die zentrale Prozessoreinrichtung (12) für jedes Terminal (16) den Risikowert über zwei Zeitintervalle unterschiedlicher Länge berechnet, um festzustellen, ob die Off-line-Betriebsart-Geschäftsgenehmigungsinformation geändert werden sollte.

3. System nach Anspruch 1, dadurch gekennzeichnet, daß die zentrale Prozessoreinrichtung (12) den Risikowert für jedes Terminal (16) durch Vergleichen der Geschäftsaufzeichnung des Terminals (16) mit Information über Konten, die den Geschäften in der Aufzeichnung zugeordnet sind, berechnet.

4. System nach Anspruch 1, dadurch gekennzeichnet, daß das Netzwerk (10) in der Lage ist, aufgrund der Verwendung von Geschäftskarten zu arbeiten, wobei jede Geschäftskarte eine Kontonummer hat, und daß jedes Terminal (16) so ausgebildet ist, daß einer der Tests (64) beinhaltet, einen Vergleich des Geschäftsbetrages, der für ein Geschäft präsentiert wird, mit einem in der Genehmigungsinformation enthaltenen Geschäftsgrenzwert vorzunehmen, und, wenn der Geschäftsbetrag den Geschäftsgrenzwert übersteigt, das Terminal (16) eine Genehmigungsanforderung an die zentrale Prozessoreinrichtung (12) sendet, und, wenn die angeforderte Genehmigung abgelehnt wird, das Terminal (16) die Kontonummer der Geschäftskarte, die für dieses Geschäft präsentiert worden ist, in eine Liste (44) in der Speichereinrichtung (40) einträgt.

5. System nach Anspruch 4, dadurch gekennzeichnet, daß jedes Terminal (16) so ausgebildet ist, daß einer der Tests (64) beinhaltet, die Kontonummer einer Geschäftskarte, die für ein Geschäft präsentiert wird, mit der Liste (44) und mit einer weiteren Liste (46) von Kontonummern von Geschäftskarten zu vergleichen, wobei die weitere Liste (46) in der Speichereinrichtung (40) gespeichert ist, und daß, wenn (52) der Geschäftsbetrag nicht größer als der Geschäftsgrenzwert ist, der in der Genehmigungsinformation enthalten ist, und (64) die Kontonummer der präsentierten Geschäftskarte nicht in der Liste enthalten ist, das Terminal (16) die Kontonummer der für dieses Geschäft präsentierten Geschäftskarte in die weitere Liste (46) in der Speichereinrichtung (40) einträgt (68), so daß eine anschließende Benutzung dieser Geschäftskarte an diesem Terminal (16) dazu führen wird, daß das Terminal (16) eine Anforderung zur Genehmigung an die zentrale Prozessoreinrichtung (12) sendet.

6. System nach Anspruch 4 oder 5, dadurch gekennzeichnet, daß jedes Terminal (16) so ausgebildet ist, daß die maximale Anzahl von Karten, die in der Liste existieren kann, fest ist, und daß, wenn dieser Grenzwert erreicht wird, die älteste Kontonummer in der Liste gelöscht wird, um Raum für die nächste in die Liste einzutragende Kontonummer zu schaffen.

7. Verfahren zum Betreiben eines Systems zum Genehmigen von Geschäften, wobei das System ein Geschäftsgenehmigungsnetzwerk (10) umfaßt, das einen zentralen Prozessor (12) hat, der mit mehreren entfernten Geschäftsterminals (16) ver-

kehrt, wobei das Verfahren beinhaltet, für jedes Terminal (16) folgende Schritte auszuführen:

Empfangen und Speichern von Genehmigungsinformation für Geschäfte in Off-line-Betriebsart an dem Ort des entfernten Terminals (16);
Betreiben des Terminals (16) in einer Off-line-Betriebsart, um ein Geschäft an ihm zu genehmigen, wenn das Geschäft Tests besteht, die durch das Terminal (16) auf der Basis der gespeicherten Genehmigungsinformation durchgeführt werden; und
Steuern des Off-line-Betriebes des Terminals (16) durch die Schritte: Erzeugen einer Aufzeichnung von durch das Terminal (16) gehandhabten Geschäften in dem Terminal (16); Senden der Geschäftsaufzeichnung von dem Terminal (16) zu dem zentralen Prozessor (12); und Berechnen eines Risikowertes, der der aus dem Terminal (16) empfangenen Geschäftsaufzeichnung zugeordnet ist, in dem zentralen Prozessor (12), und, wenn sich der berechnete Risikowert von einem gewünschten Risikowert unterscheidet, Senden einer neuen Off-line-Betriebsart-Geschäftsgenehmigungsinformation zu dem Terminal (16), die so ausgewählt wird, daß der Risikowert in dem Terminal (16) auf den gewünschten Risikowert eingestellt wird.

8. Verfahren nach Anspruch 7, dadurch gekennzeichnet, daß der Risikowert über zwei Zeitintervalle unterschiedlicher Länge berechnet wird, um festzustellen, ob der Geschäftsgrenzwert geändert werden sollte.

9. Verfahren nach Anspruch 7, dadurch gekennzeichnet, daß der Risikowert durch Vergleichen der Geschäftsaufzeichnung mit Information über den Geschäften zugeordnete Konten berechnet wird.

10. Verfahren nach Anspruch 7, dadurch gekennzeichnet, daß die Geschäfte auf der Basis der Benutzung von Geschäftskarten genehmigt werden, wobei jede Geschäftskarte eine Kontonummer hat; und das für jedes entfernte Terminal (16):
die an dem Ort des Terminals (16) gespeicherte Genehmigungsinformation mehrere Listen (42, 44, 46) von Kontonummern umfaßt; und
der Betrieb des Terminals (16) die Schritte beinhaltet:

Vergleichen der Kontonummer der für ein Geschäft präsentierten Karte mit einer ersten gespeicherten Liste (42) von ungültigen Kontonummern;
Anfordern einer Genehmigung bei dem zentralen Prozessor (12) für Geschäfte, die gewisse Tests (52, 64) auf der Basis der gespeicherten Genehmigungsinformation nicht bestehen, einschließlich eines Tests (64) auf Nichtvorhandensein der Kontonummer in einer zweiten gespeicherten Liste (44); und
wenn irgendeine derartige verlangte Genehmigung abgelehnt wird (58), Eintragen der Kontonummer der für dieses Geschäft präsentierten Geschäftskarte in die zweite gespeicherte Liste (44), so daß eine spätere Benutzung dieser Geschäftskarte an dem Terminal (16) dazu führen wird, daß das Terminal (16) direkt eine Genehmigung bei dem zentralen Prozessor (12) anfordert, selbst wenn der Rest (50, 52) der Tests auf der Basis der Geschäftsinformation bestanden wird.

11. Verfahren nach Anspruch 10, dadurch gekennzeichnet, daß der Betrieb jedes Terminals (16) die Schritte umfaßt:
wenn alle Tests (50, 52, 64) auf der Basis von in dem Terminal (16) gespeicherter Genehmigungsinformation bestanden werden, Eintragen der Kontonummer der für dieses Geschäft präsentierten Geschäftskarte in eine dritte gespeicherte Liste (46), so daß ein späterer Gebrauch dieser Geschäftskarte an diesem Terminal dazu führen wird, daß das Terminal direkt eine Genehmigung von dem zentralen Prozessor (12) verlangt, wenn der Rest (50, 52) der Tests auf der Basis der Genehmigungsinformation bestanden wird, wobei die Tests einen Test (64) auf Nichtvorhandensein der Kontonummer in der dritten gespeicherten Liste (46) umfassen.

12. Verfahren nach einem der Ansprüche 7 bis 11, dadurch gekennzeichnet, daß die Genehmigungsinformation einen Geschäftsgrenzwert umfaßt und daß die Auswahl der neuen Off-line-Betriebsart-Geschäftsgenehmigungsinformation die Berechnung eines neuen Geschäftsgrenzwertes beinhaltet, der den Risikowert an dem Terminal (16) auf den gewünschten Risikowert einstellt.

Revendications

1. Système d'autorisation de transactions, système comprenant un réseau d'acceptation de transactions (10) possédant un moyen de centre de traitement (12) pour la réception et l'analyse des enregistrements de transactions pour chaque poste d'une pluralité de terminaux de transaction à distance (16) prévus pour communiquer avec le moyen de centre de traitement (12) via le réseau (10), chaque terminal de transaction (16) étant prévu pour autoriser des transactions en mode local qui satisfont à des tests effectués par le terminal (16) sur la

base d'une information d'autorisation conservée dans le moyen de stockage prévu à cet effet, et le terminal (16) étant prévu, de plus, pour stocker dans le moyen de stockage un enregistrement des transactions traitées par le terminal (16) et possédant un moyen d'émission et de réception associé pour la réception d'une information et pour l'émission d'une information vers le moyen de centre de traitement (12), l'information transmise au moyen de centre de traitement (12) comprenant l'enregistrement des transactions dans le terminal (16), et le moyen de centre de traitement (12) étant prévu pour commander le mode en local de chaque terminal (16) en calculant un niveau de risque associé à l'enregistrement des transactions du terminal (16) et, si le niveau de risque calculé diffère d'un niveau de risque désiré, en émettant vers le terminal (16) une nouvelle information d'autorisation de transaction, en mode local, sélectionnée pour régler le niveau de risque sur le terminal (16) sur le niveau de risque désiré.

2. Système selon la revendication 1, caractérisé en ce que ledit moyen de centre de traitement (12) calcule pour chaque terminal (16) le niveau de risque sur deux intervalles de temps de longueurs différentes afin de déterminer si l'information d'autorisation de transaction en mode local doit être modifiée.

3. Système selon la revendication 1, caractérisé en ce que le moyen de centre de traitement (12) calcule le niveau de risque pour chaque terminal (16) en comparant l'enregistrement des transactions du terminal (16) avec une information sur les comptes associés aux transactions dans l'enregistrement.

4. Système selon la revendication 1, caractérisé en ce que le réseau (10) est prévu pour fonctionner en réponse à l'utilisation de cartes de transaction, chaque carte de transaction possédant un numéro de compte, et en ce que chaque terminal (16) est tel qu'un desdits tests (64) comprend une comparaison du montant de transaction présenté pour une transaction avec une limite de transaction incluse dans l'information d'autorisation et, si le montant de la transaction dépasse la limite de transaction, le terminal (16) émet une demande d'autorisation vers le moyen de centre de traitement (12), et si une telle demande d'autorisation est refusée, le terminal (16) ajoute le numéro de compte de la carte de transaction présentée pour cette transaction à une liste (44) dans ledit moyen de stockage (40).

5. Système selon la revendication 4, caractérisé en ce que chaque terminal (16) est tel qu'un desdits tests (64) comprend la comparaison du numéro de compte d'une carte de transaction présentée pour une transaction avec ladite liste (44) et une liste supplémentaire (46) de numéros de compte des cartes de transaction, ladite liste supplémentaire (46) étant stockée dans ledit moyen de stockage (40), et que, si (52) le montant de la transaction n'est pas supérieur à la limite de transaction incluse dans ladite information d'autorisation et (64) le numéro de compte de la carte de transaction présentée n'est pas présent dans lesdites listes, le terminal (16) ajoute (68) le numéro de compte de la carte de transaction présentée pour cette transaction à ladite liste supplémentaire (46) dans ledit moyen de stockage (40) de telle façon qu'une utilisation suivante de cette carte de transaction sur ce terminal (16) entraîne une transmission par le terminal (16) d'une demande d'autorisation vers ledit moyen de centre de traitement (12).

6. Système selon la revendication 4 ou 5, caractérisé en ce que chaque terminal (16) est tel que le nombre maximum de cartes pouvant exister dans la liste est fixé et lorsque cette limite est atteinte, le numéro de compte le plus ancien de la liste est effacé pour faire de la place pour le numéro de compte suivant à ajouter à la liste.

7. Procédé de fonctionnement d'un système pour l'autorisation de transactions, le système comprenant un réseau d'acceptation de transaction (10) possédant un centre de traitement (12) communiquant avec une pluralité de postes de transactions à distance (16), procédé comprenant, pour chaque terminal (16), les étapes suivantes:

- la réception et le stockage sur la position du terminal à distance (16) d'une information d'autorisation pour des transactions en mode local;

- le fonctionnement du terminal (16) en mode local afin d'autoriser une transaction si la transaction satisfait aux tests effectués par le terminal (16) sur la base de l'information d'autorisation stockée;

et commandant le mode en local de fonctionnement du terminal (16) selon les étapes suivantes :

- la production dans le terminal (16) d'un enregistrement de transactions maniées par le terminal (16);

- la transmission de l'enregistrement des transactions du terminal (16) vers le centre de traitement (12); et

- le calcul dans le centre de traitement (12) d'un niveau de risque associé à l'enregistrement des transactions reçu du terminal (16) et si le

niveau calculé de risque diffère d'un niveau de risque désiré, la transmission au terminal (16) d'une nouvelle information d'autorisation de transaction, en mode local, sélectionnée pour régler le niveau de risque au terminal (16) sur le niveau de risque désiré.

8. Procédé selon la revendication 7, caractérisé en ce que le niveau de risque est calculé sur deux intervalles de temps de longueurs différentes afin de déterminer si la limite de transaction doit être modifiée.

9. Procédé selon la revendication 7, caractérisé en ce que le niveau de risque est calculé en comparant l'enregistrement des transactions avec une information sur les comptes associés aux transactions.

10. Procédé selon la revendication 7, caractérisé en ce que les transactions sont autorisées sur la base de l'utilisation des cartes de transaction, chaque carte de transaction possédant un numéro de compte, et en ce que, pour chaque terminal à distance (16) :

- l'information d'autorisation stockée sur la position du terminal (16) comprend une pluralité de listes (42, 44, 46) de numéros de comptes;

et le fonctionnement du poste (16) comprend les étapes suivantes :

- la comparaison du numéro de compte de la carte présentée pour une transaction avec une première liste stockée (42) de numéros de comptes non valides;

- la demande d'une autorisation à partir du centre de traitement (12) pour des transactions qui n'ont pas passé certains tests (52, 64) sur la base de l'information d'autorisation stockée, comprenant un test (64) sur l'absence du numéro de compte dans une seconde liste stockée (44); et

- si une quelconque telle demande d'autorisation est refusée (58), l'addition du numéro de compte de la carte de transaction présentée pour cette transaction à ladite seconde liste stockée (44) de telle façon qu'une utilisation suivante de cette carte de transaction sur le terminal (16) entraîne un passage du terminal (16) en ligne afin de demander une autorisation au centre de traitement (12) même si le reste (50, 52) des tests sur la base de l'information d'autorisation sont satisfaits.

11. Procédé selon la revendication 10, caractérisé en ce que le fonctionnement sur chaque terminal (16) comprend l'étape suivante :

si tous les tests (50, 52, 64) basés sur l'information d'autorisation stockée dans le terminal (16) sont satisfaits, l'addition du numéro de compte de la carte de transaction présentée pour cette transaction à une troisième liste stockée (46) de telle façon qu'une utilisation suivante de cette carte de transaction sur ce terminal entraîne le passage en ligne du terminal afin de demander une autorisation au centre de traitement (12) si le reste (50, 52) des tests sur la base de l'information d'autorisation sont satisfaits, lesdits tests comprenant un test (64) sur l'absence du numéro de compte dans la troisième liste stockée (46).

12. Procédé selon l'une quelconque des revendications 7 à 11, caractérisé en ce l'information d'autorisation comprend une limite de transaction et en ce que la sélection de ladite nouvelle information d'autorisation de transaction en mode local comprend le calcul d'une nouvelle limite de transaction réglant le niveau de risque dans le terminal (16) sur le niveau de risque désiré.

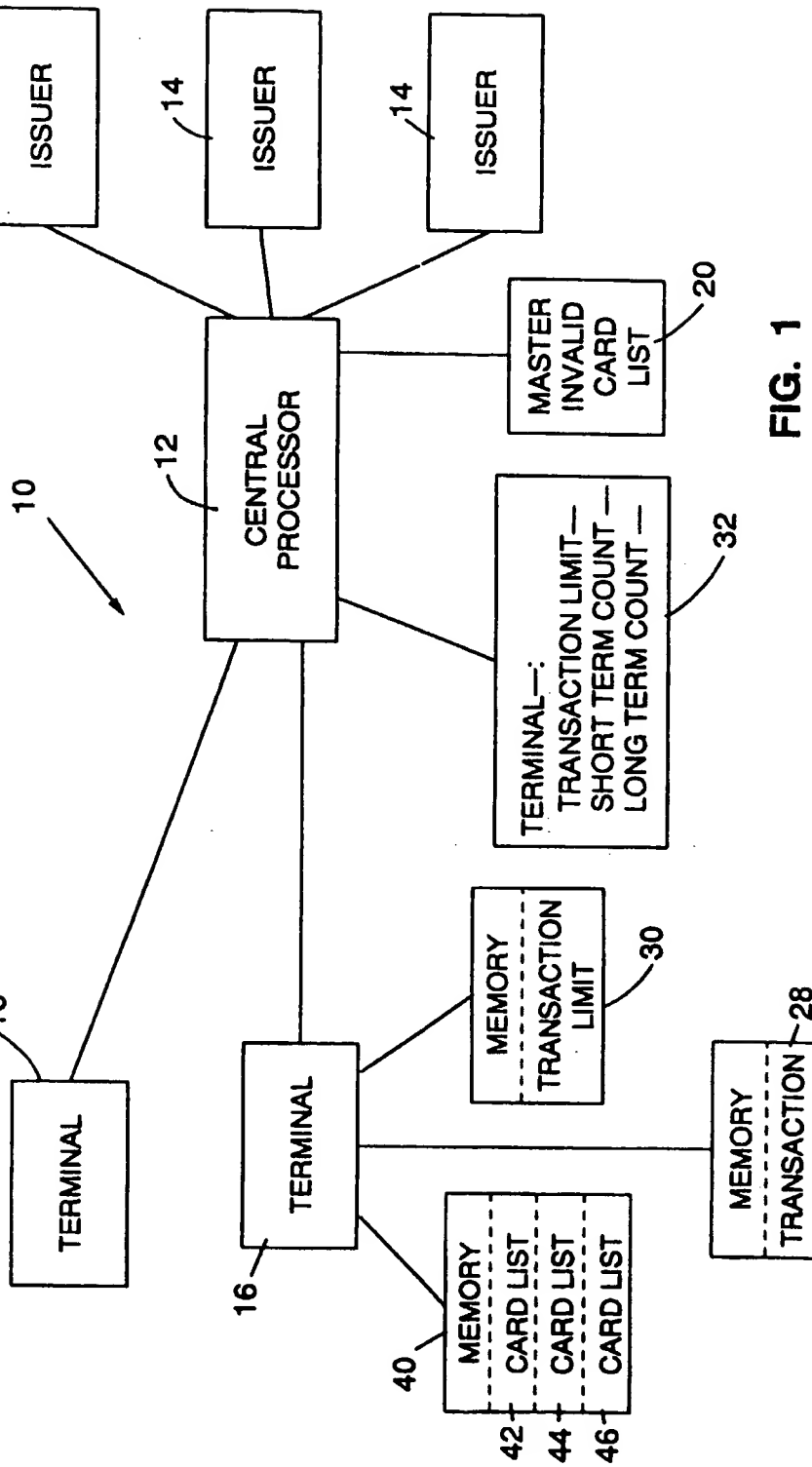
ISSUER
14
ISSUER
14
ISSUER
14
MASTER INVALID CARD LIST
20
CENTRAL PROCESSOR
12
10
TERMINAL—: TRANSACTION LIMIT— SHORT TERM COUNT— LONG TERM COUNT—
32
TERMINAL
16
MEMORY TRANSACTION LIMIT
30
MEMORY TRANSACTION RECORD
28
TERMINAL
16
MEMORY CARD LIST CARD LIST CARD LIST
40
42
44
46

FIG. 1

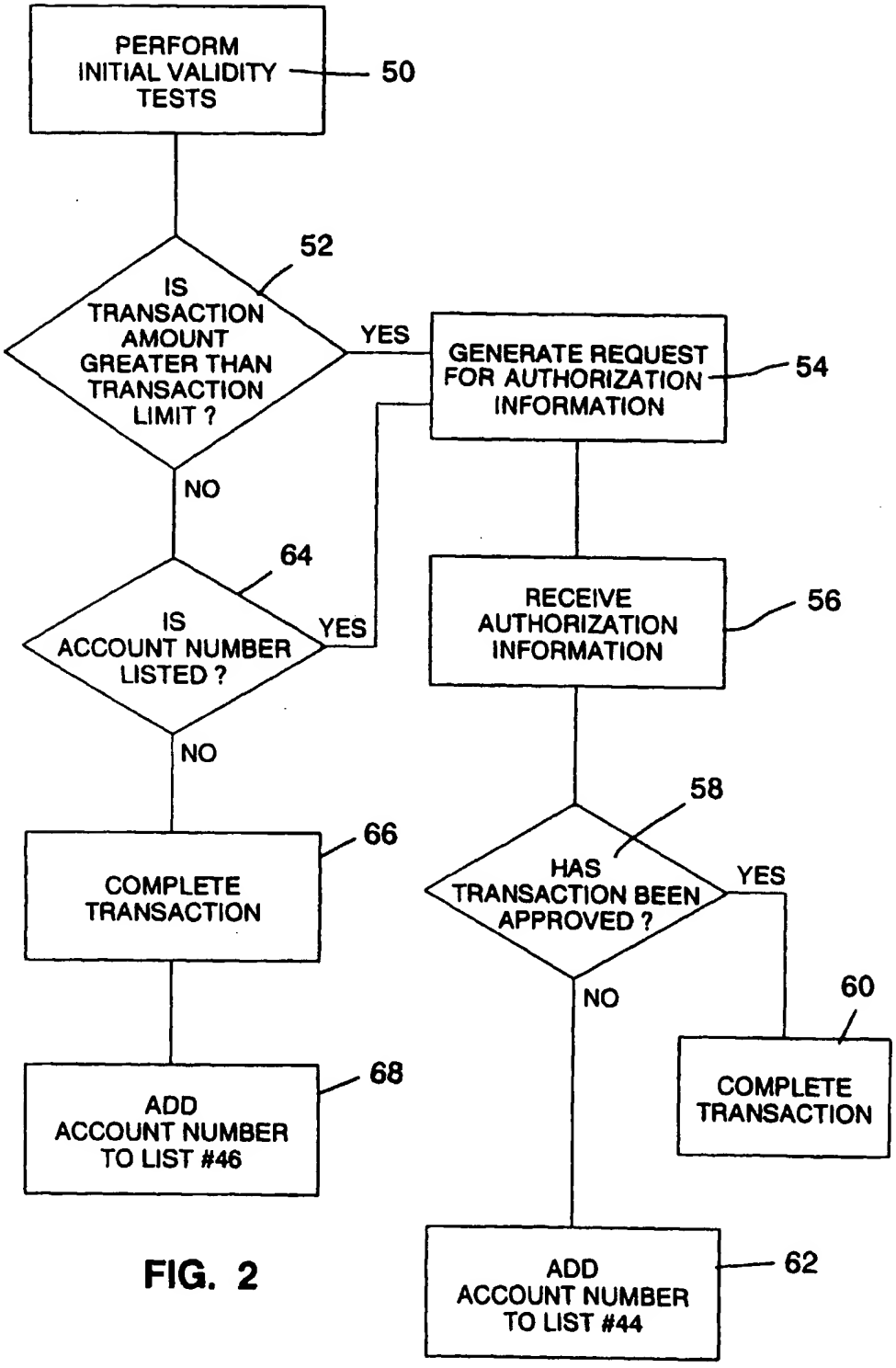
PERFORM INITIAL VALIDITY TESTS
50
IS TRANSACTION AMOUNT GREATER THAN TRANSACTION LIMIT ?
52
YES
GENERATE REQUEST FOR AUTHORIZATION INFORMATION
54
NO
IS ACCOUNT NUMBER LISTED ?
64
YES
RECEIVE AUTHORIZATION INFORMATION
56
NO
HAS TRANSACTION BEEN APPROVED ?
58
YES
NO
COMPLETE TRANSACTION
66
COMPLETE TRANSACTION
60
ADD ACCOUNT NUMBER TO LIST #46
68
ADD ACCOUNT NUMBER TO LIST #44
62

FIG. 2